Handling and Reporting Information Security Incidents

A Handbook for Employees

Rev: 6/2001

Published by:
Information Security Unit
Office of Compliance
Department of Corrections
State of California

Draft

Information Security Reporting Handbook
Rev: July 2001

Quick Telephone Reference

Supervisor	_____
Unit Manager	_____
Information Security Coordinator	_____
Information Security Officer	(916) 358-2459

Draft

Table of Contents

Information Security Reporting Handbook
Rev: July 2001

Notes

Draft

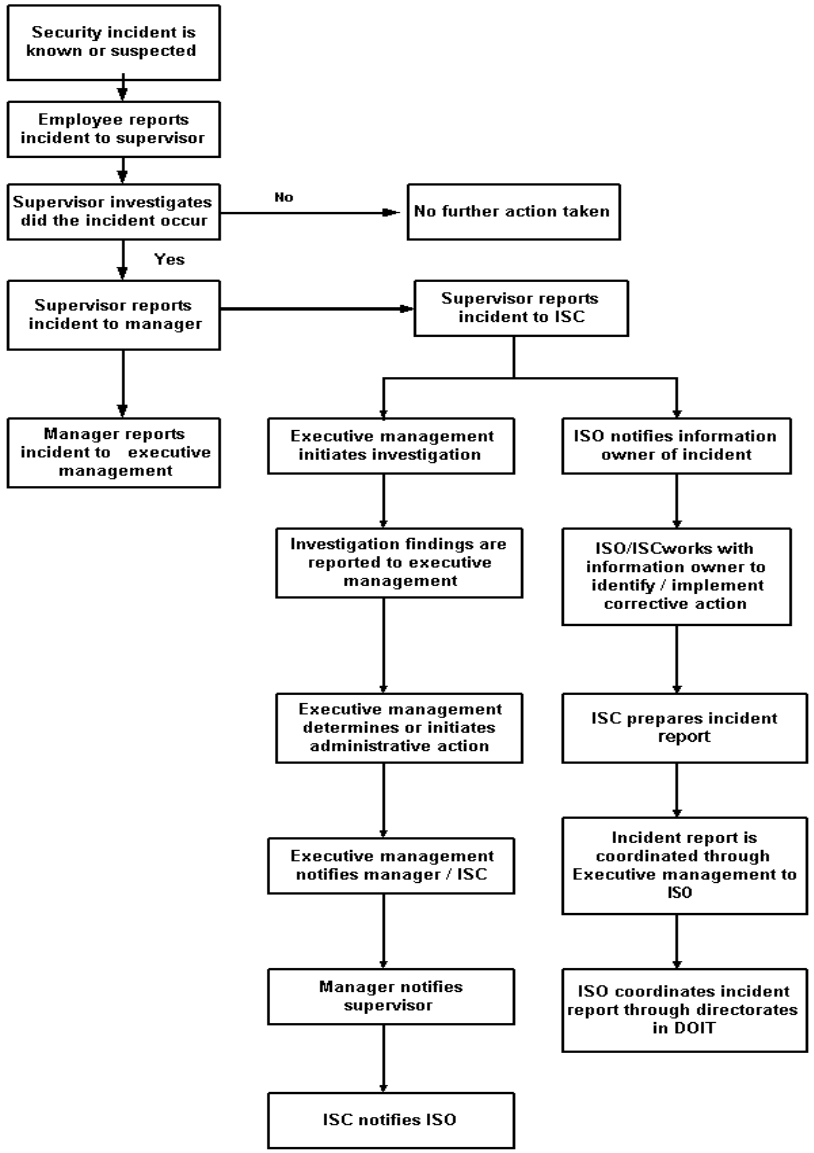
Draft

Introduction

The purpose of this handbook is to provide guidance in recognizing and reporting breach's in security in information processing handling systems. For the purposes of this handbook information handling system consist of input documents, computer-processing systems, including computer networks and any associated peripheral device, and computer printouts or reports.

A security breach is the improper modification, destruction, or disclosure of information, weather by accident or deliberately to an individual that is not authorized to receive that information. A security breach can also consist of the modification or destruction of information handling systems, communication networks, and computer programs.

The purpose of reporting security incidents promptly is to provide an opportunity to warn others of the problem. Additionally, it provides the opportunity to determine what changes should be made to future policies and procedures to avoid a reoccurrence of the problem, and in general, improved information handling systems processes.



Office of Personnel Management

The Office of Personnel Management will ensure consistency among administrative actions taken for similar types of information security incidents.

Glossary of Terms

The glossary of terms can be found on the Intranet or Internet by go to the CDC security web-site. The glossary will by navigating to a section listed as Glossary. The Intranet can be accessed by through your Internet browser by entering **Intranet** on the address bar. The Internet address for the CDC Security web-site is: www.cdc.state.ca.us/ISU/index.htm

Reporting A Security Incident

What should be reported.

If you believe that an information security incident has occurred, report it to your supervisor at once. Various types of information security incidents are described starting on page _____

What needs to be reported about the incident?

Both the Information Security Officer and the Department of Information Technology require specific information. Those investigating the incident require additional details. See evidence gathering, Page _____ of this handbook, for the specific information needed.

How should the incident be reported?

For quick reference, see the Incident Reporting Flow Diagram, Page _____ of this handbook, see Roles and responsibilities page _____ of this Handbook, and for instructions on how to complete and Incident Report, See Page _____.

Time Frame for Reporting Security Incidents

Security incidents must be reported within five (5) days of recognition that a security incident has occurred.

Because of the short time frame required for reporting an incident, some incident reports may not contain all of the information listed in the report form. Also, the investigation may not be completed, in fact, may not even be started, before the incident report is

prepared. Information Security Coordinators should provide as much of the information as possible and should enter N/A (not available) in those areas where the information is not yet known. When an item of information is not known at the time of filing the report with the ISO, a supplemental report must be prepared when the information becomes available.

Forms

To assist in the preparation of a Security Incident Report we are making the forms available online, simply **CLICK HERE.**

Information You Will Need To Gather

Both the Information Security Officer and the Department of Information technology require the following information.

Information Required by CDC

1. The name of the :
   Institution,
   Parole Office,
   Parole Region, or
   Headquarters Ofc.
2. Name of the Warden or Supervisor
3. Name of the Information Security Coordinator (ISC)
4. Address of the ISC
5. Telephone number of the ISC

Information required by both CDC and DOIT

1. Date and time if the incident
2. Incident was reported to.
3. Date and time incident was reported to the supervisor.

1. incident handling and reporting process. 2) Handle all legislative contacts.

Managers and Supervisors

Managers, supervisors, and the management of contractors, consultants, and external CDC information users will:

1. Ensure that their employees know how to identify and report incidents.
2. Ensure that their employees identify and report incidents involving CDC information assets.
3. Conduct an initial investigation of suspected incidents to determine whether they are or appear to be actual incidents.
4. Report all incidents to executive management via the reporting chain-of-command.
5. Preserve evidence.
6. Remove suspected employees from sensitive job duties until an investigation is conducted and the employee's involvement is determined.6). Cooperate with investigators and law enforcement personnel during investigations.

Network Administrators

Network Administrators are in a position to identify symptoms of security problems that may go unnoticed by individual users of the system. They are to report such activity to the impacted management entity and the ISO.
Office of Communications

The Office of Communications will:

1. Handle all media contacts regarding information security incidents.
2. Prepare any necessary press releases pertaining to information security incidents.

1. Provide assistance and guidance, as appropriate, to management, ISCs, and employees concerning the handling and reporting of incidents.
2. Ensure timely notification to the Directorate, and other key departmental personnel, when information security incidents of significant impact occur.
3. In accordance with SAM requirements, file an Information Security Incident Report with DOIT, within ten (10) working days of discovery of the incident.
4. Update the incident handling process as necessary.
5. Report incidents that may involve a violation of the Information Practices Act to the departmental Information Practices Act Coordinator.
6. Inform Information Owners of information security incidents that involve the information assets for which they have responsibility.
7. Provide assistance or guidance with training programs to teach users how to identify incidents.

Information Systems Unit

The Information Systems Unit will:
1. Notify the ISO, ISC, and impacted management of any activity or problems that may indicate a possible security incident.
2. Implement automated or technological controls identified by the ISO, ISC, and/or Information Owner.

Legislative Office

The Legislative Office will:
Notify the ISO of any new or pending legislation that may have an impact on the Department's information security

4. Name and phone number of the supervisor.
5. Incident was reported to (law enforcement?)
6. Description of the indent, including:
   a) Type of incident
   b) Sequence of events, and
   c) Internal controls that failed, if known
   d) Means of discovery
7. Estimated cost of the incident
   a) Hardware (replacement value)
   b) Software (replacement value)
   c) Lost personnel time
   d) Work contracted out during interruptions, and
   e) Personnel time required to restore to operational condition.
8. Factors included in the cost estimate
9. Corrective actions taken, or that will be taken, to prevent further occurrences.
10. Estimated cost of corrective actions.
11. Factors included in estimated cost.
12. Will criminal charges be files? If so, under what code section
13. What other administrative actions will be taken against those who were responsible for the incident.

In addition to the foregoing, the following information will be required by the investigating entity.

1. Which record(s) or files(s) were accessed?
2. Was the access seemingly part of a routine job or was it unusual in its circumstances?
3. Identification of the terminals(s) or computer(s) which were used in the security incident.
4. Name of the person(s) who may have committed the security breach, if known.
5. Name(s) and work location(s) of witness.

If an inmate was involved the following information will also be required.

1. Name of the inmate's supervisor.
2. Location of the inmate's work area.
3. DOM policy/Procedure that were violated.

Submitting an Incident Report

1. The witness to the incident reports it to the unit supervisor.

2. The supervisor performs a preliminary investigation to confirm that an incident has probably occurred. If it appears as if an incident probably has occurred, the supervisor reports it to the manager and the Information Security Coordinator (ISC).

3. The ISC reports the incident to the ISO.

4. The ISO notifies the Information Owner of the incident.

5. The manager reports the incident to the impacted Deputy Director(s), Assistant Director(s), Warden(s), or Regional Administrator(s).

6. The Deputy Director, Assistant Director, Warden, or Regional Administrator initiates an investigation by the appropriate entity.

The ISC prepares the Information Security Incident Report and coordinates it through the Deputy Director or Assistant Director to the ISO. If an institution or parole office is involved, the ISC prepares the report and coordinates it via the

1. Provide guidance and assistance in determining the appropriate action regarding incidents involving a violation of the Information Practices Act.

Information Security Coordinators

The Information Security Coordinator will:
1. Coordinate incident reports for their division, institution, or parole region.
2. Provide assistance to investigative entities as requested.
3. Report incidents to the ISO within five (5) working days of discovery of the incident.
4. Provide assistance and guidance, as needed, to employees concerning the handling of incidents within their division, institution, or parole region.
5. Upon notification from executive management, notify the ISO of incident investigation findings.
6. Communicate to the ISO changes needed in the incident handling process.
7. As part of the basic information security awareness training class, train employees within their division, institution, or parole region in recognizing and reporting incidents.
8. As necessary, work with the Information Owner, ISO, ISCs, and management to identify controls needed to prevent the recurrence of an incident.

Information Security Officer

The ISO, located in the Office of Compliance, will:
8. Function as the Department's internal source of information concerning incidents.
9. Provide assistance to investigative entities as requested.

Executive Management (Deputy Directors, Assistant Directors, Wardens, Regional Administrators)

Executive managers will:

1. Ensure that external CDC information users or contractors, authorized by them to access departmental information assets, are advised of their responsibilities.
2. When appropriate, request a formal investigation of incidents.
3. Keep the impacted unit's manager apprised of the status and/or findings of incident investigation.
4. Notify ISC of incident investigation findings.
5. Determine appropriate administrative action.
6. Ensure that such action is taken.
7. Ensure that appropriate administrative action is taken against those external CDC information users or contractors who are responsible for an information security incident.

Information Owners

Information Owners will:

1. Help determine revisions needed to policies and procedures and the system or technological controls needed to prevent a recurrence of an incident.
2. Advise the appropriate executive manager, ISC, and ISO of corrective measures to be implemented and the status of the implementation plan.

Information Practices Act Coordinator

The Information Practices Act Coordinator will:

2. Provide guidance and assistance in determining if an incident involves a violation of the Information Practices Act.

Information Security Reporting Handbook
Rev: July 2001

7. Warden or Regional Administrator to the Deputy Director to the ISO.

8. The ISO coordinates the incident report through the Directorate to DOIT, if appropriate.

9. The investigative entity performs an investigation, in cooperation with law enforcement agencies, if appropriate. At the conclusion of the investigation, the investigative entity reports the findings to the Deputy Director, Assistant Director, Warden, or Regional Administrator, who determines the appropriate action.

10. The Deputy Director, Assistant Director, Warden, or Regional Administrator notifies the Manager and the ISC of the investigation findings.

11. The ISC notifies the ISO of the investigation findings.

12. The ISC and ISO work with the information owner to ensure that appropriate corrective measures are identified and implemented to prevent a recurrence of the incident

Evidence Gathering

Suspected incidents should be confirmed, insofar as possible, by the supervisor. All potential evidence and witnesses should be identified. Care must be taken to preserve the evidence for use by investigators and prosecutors. If criminal activity is suspected and the suspect is a CDC employee, student, contractor, consultant, or any other employee utilizing CDC facilities, the suspect will be interviewed by the appropriate CDC management entity.

POLICY

Legal
Both the United States and California constitution guarantee the peoples right to privacy. Although the Federal Freedom of Information Act and the California Public Records Act (GC 6251-6255) mandate universal accessibility to public records, the Public Records Act exempts certain records from unauthorized disclosure (GC 6254) and provides for protection of an agency's proprietary data (GC 6255).

The California Penal Code 502 specifies types of computer related crimes and associated penalties.

The Federal Copyright law provides protection to software publishers from software copyright infringement.

Departmental Operations Manual (DOM), Volume IV, Section 49010.6.2:

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. It is the policy of the Department that the following incidents shall be reported through the chain-of-command to the departmental ISO:

- Any incident involving unauthorized access to automated data, automated files, or databases.
- Any incident involving the unauthorized modification, destruction, or loss of automated data, automated files, or databases.
- Any incident involving a virus or other such malicious computer code.
- Any incident involving the unauthorized use of computer equipment, automated data, automated files, or databases.

Roles and Responsibilities

The persons and organizations listed below in alphabetical order have specific responsibilities with regard to the reporting and handling of information security incidents. It is important for each entity to know in advance its role.

Audit Groups

Groups responsible for auditing departmental operations and external CDC information users will:

1. Report to the Deputy Director, Assistant Director, Warden, or Regional Administrator of the impacted division, institution, or parole region, incidents discovered during their audits, and identify administrative and system control problems.
2. Recommend solutions to the appropriate executive management, ISC, and ISO.

Employees and Other CDC Information Users

All CDC employees, students, consultants, contractors, and employees of external CDC information users will:

1. Report to their supervisor or manager suspected or known incidents.
2. Preserve evidence.
3. Cooperate with investigative and law enforcement personnel during investigations.

Theft of information, computer equipment, or information services includes, but is not limited to:

1. Unauthorized removal of computers, peripherals, or computer system parts from CDC premises without written permission from the employee's supervisor.
2. Unauthorized removal of floppy diskettes.
3. Unauthorized removal of CDC software and system documentation.
4. Unauthorized use of CDC information services includes, but is not limited to:
    - Using a CDC computer for personal reasons without the supervisor's approval.
    - Using a CDC computer for an outside business or interest.
5. Copying CDC-owned software for personal use.

- Any incident involving the misuse of the information assets of the Department.

State Administrative Manual (SAM), Section 4845:

INCIDENT REPORTS—Agency management must promptly investigate incidents involving the unauthorized or accidental modification, destruction, disclosure, loss, or access to automated files and data bases, as well as incidents involving loss, damage, or misuse of information assets. If there is a possibility that an incident constitutes a criminal act, the agency must notify the California Highway Patrol and other appropriate law enforcement agencies. In addition, each agency having ownership responsibility for information (SAM Section 4841.4) must complete an Information Security Incident Report. The report, signed by the agency director and Information Security Officer, must be submitted to the Office of Information Technology within ten working days of the agency's becoming aware of an incident involving one or more of the following.

1. Unauthorized intentional release, modification, or destruction of confidential or sensitive information or the theft of such information, including information stolen in conjunction with the theft of a computer or data storage device;
2. Use of a State information asset in commission of a crime;
4. Tampering, interference, damage, or unauthorized access to computer data and computer systems as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502;
5. Intentional non-compliance by the custodian of information with their responsibilities as defined in SAM Section 4841.6; or

6. Intentional damage or destruction of State information assets, or the theft of such assets, with an estimated value in excess of $2,500.

Definition

An information security incident is an event involving:

1. unauthorized modification, distribution, or destruction of automated or manual information;
2. unauthorized disclosure of or access to automated or manual information; or
3. loss of, damage to, or misuse of information assets.

Definitions for terms used in this information security incident reporting guide can be found in the Glossary. Accidental keying and unintentional transaction requests that are immediately canceled are exempt from this definition.
A suspicion alone does not constitute an incident. However, if, after a preliminary investigation by the supervisor, the event appears to be an information security incident, it should be reported in accordance with the incident reporting procedures in this guide.

Purpose

The purpose of this policy is to ensure the continued availability and integrity of the California Department of Corrections' (CDC's) information assets. Further, this policy is to ensure compliance with the information security incident reporting requirements in the SAM, and to define the roles and processes for handling and reporting information security incidents. Standards
Information security incidents will be handled in a manner that meets the following standards:

Reportable incidents of destruction or damage include deliberate, or through negligence, damage to or destruction of manual or computerized information, computer programs, computer hardware, computer peripherals such as printers, or computer networks.

Examples of incidents of destruction or damage to information assets include, but are not limited to:
1. Damage to computer equipment caused by sabotage.
2. Damage to computer equipment caused by water, coffee, or other liquid spills, food particles, etc.
3. Physical damage to system documentation due to negligence (hard copies of computer programs, system manuals, etc.).
4. Destruction of or damage to magnetic tapes due to negligence.
5. Erasure of data from a hard drive, tape, or other storage system.
6. Damage to or loss of files or programs due to the installation of unauthorized software.
7. Intentional unauthorized physical destruction of all or part of a CDC document.

Theft of Information, Computer Equipment, or Information Services

Employees taking home CDC computer equipment must have written permission from their supervisor. The unit manager must keep a record of each unit's loaned equipment on file.

Information services is defined as including, but not being limited to, computer time, information processing, storage, or other uses of a computer, computer system (including peripherals such as printers and modems), or a computer network.

by contacting their immediate supervisor. If they do not, you should immediately treat the event as an information security incident and initiate the procedures outlined in this guide. If unsure, ask your supervisor before taking any action.

All computer users should learn to recognize symptoms that may indicate malicious code or hacker invasion. Refer to the CDC Information Security Awareness Handbook for Employees for a complete description of these symptoms and instructions for what to do.

Examples of incidents of malicious code include, but are not limited to:

1. An employee brings in work from home on a virus-infected diskette.
2. A repair technician uses a virus-infected diagnostic diskette to repair a computer.
3. An employee receives an electronic mail message with a virus-infected word processing document attached.

Examples of incidents of hacker intrusion include, but are not limited to:

1. A person calling, claiming to have the authority to request information from a database or computer system.
2. A person claiming to be a Network Administrator asks for an employee's network User ID and password in order to perform troubleshooting on the network.

Destruction and Damage to Information Assets

Note: Destruction and damage of data by viruses or hackers is covered in the Malicious Code and crackers Section.

1. Keep unnecessary adverse consequences to CDC's resources, employees, and customers to a minimum.
2. Discourages repetition of incidents.
3. Meets reporting requirements specified in the SAM.
4. Assures that all perpetrators are prosecuted to the full extent of the law.
5. Provides feedback to assist the ISO, Information Security Coordinators (ISCs), and management in identifying and correcting inadequacies in the Department's Information Security

Standards

Information security incidents will be handled in a manner that meets the following standards.

1. Keep unnecessary adverse consequences to CDC's resources, employees, and customers to a minimum.
2. Discourage the repetition of incidents
3. Meets reporting requirements in the State Administrative Manual.
4. Assures that all perpetrators are prosecuted to the full extent of the law; and
5. Provides feedback to assist the ISO, information Security Coordinators (ISCs) and management in identifying and correcting inadequacies in the Departments Information Security Program.

Program Impact on Departmental Operations

This policy is not intended to modify existing policies or procedures in other departmental programs, or to change existing operations other than those for responding to and reporting of information security incidents.

Types Of Information Security Incidents

Unauthorized Access

Access means entry to or communication with a computer, computer system, or network, or contact with manual or automated information. An authorized person is one whose job duties require specified access to CDC information assets. Unauthorized Access is access by a person whose job duties do not require such access.

Most of the other types of security incidents discussed in this guide require unauthorized access before they can be perpetrated. However, because intentional unauthorized access is itself a crime, this category is not redundant. A person who obtains unauthorized access is referred to as an unauthorized person.

Examples of unauthorized access include, but are not limited to:

1. Access to a computer via another person's User ID. There are two ways in which this can occur:
   - An employee who is logged on allows another employee to use the computer or terminal without logging off. This is unauthorized access, even though the second employee may be authorized to use the system under his or her own User ID, because the second employee is not authorized to use the computer under the first employee's User ID.
   - An employee logs on using another employee's User ID.
2. Use of a CDC terminal or computer by an individual who has not been authorized to use it.
3. Helping an unauthorized person gain access to a computer, computer system, network, application, or transaction.
4. Use of a computer application by a person whose job duties do not require such use.
5. Exploration of a computer's operating system without authorization.

Information Security Reporting Handbook
Rev: July 2001

Introduction of malicious code may occur accidentally or intentionally. However, most malicious code is accidentally introduced to desktop computers by repair technician diskettes, diskettes used at educational institutions, or employees bringing files from home. In some cases, brand-name software still in shrink-wrapped packaging and new computers or hardware are virus carriers. All new programs and computers must be scanned for viruses before they are installed at CDC. If you do not have CDC-approved virus detection software on your PC, contact your PC coordinator.

A cracker (sometimes called a hacker) is a person who gains access to a computer from a remote location or to telecommunications components. Access is usually achieved by use of a modem. However, local area network cables can be tapped directly; and people in the right place at the right time can gain direct access to a computer and read the files or perpetrate other undesirable acts while on the system. It is a crime to gain unauthorized entry to a computer resource even though no alteration of data occurs.

Cracking includes breaking into a computer-controlled telephone system as well as entry into the computer's operating system programs or data storage.

Some Crackers like the challenge of calling an office and using "social engineering" (i.e., persuasion, impersonation of an authorized individual, authoritative voice, or impressive computer jargon) to gain password information or access through an authorized person. If you receive a call from a person who claims to have the authority to request information or gain access to a database or computer system. Write down their request, but do not grant it. Ask for their name, unit, position, phone number, and supervisor's name. Confirm that they do in fact have this authority

Draft

Examples of incidents of information falsification include, but are not limited to:

1. Intentional entering false data into a database or file.
2. Intentional entering incomplete data into a record without authorization.
3. Omitting entries or updates in a database, file, or record without permission.
4. Modifying or deleting valid information without authorization.
5. Changing of production data by a version of an application program which has not been formally tested and released to production via the Department's standard application change control process.
6. Modifying computer source code without authorization.
7. Modifying an operating system or network configuration without authorization.
8. Changing access permissions in an access control table without authorization.
9. Unauthorized alteration of paper documents.

Malicious Code and Hacker Intrusion

Malicious code is computer instructions, usually in the form of a program, designed to perform undesired changes to the computer system, data, or programs. The best-known and most common malicious code is a computer virus, which is code that can duplicate itself within one machine and spread to others. This is more likely to happen on a desktop computer such as a Macintosh or PC rather than on a minicomputer or mainframe. Some malicious code can destroy all functions or data on a computer—even damage or destroy the hardware itself.

6. Unauthorized use of a modem.
7. Unauthorized attachment of a workstation to a network.
8. Possession by an unauthorized person of CDC documents containing information not related to that person's job function.

Misuse of Information Assets

Misuse of information assets occurs when CDC information is read, copied, or used for purposes that are not authorized or when CDC information resources are used for unauthorized purposes. Authorized purposes include only those related to the individual's job or education assignment. External CDC information users, contractors, and consultants are allowed to read, copy, or use only those CDC information assets that pertain to their contracted CDC business and only for the purpose stated in their agreement with the Department.

One way in which an accidental viewing of information may occur is placement of computer terminals/monitors or paper documents in the work area in such a way that unauthorized employees, inmates, or parolees cannot avoid seeing them. This should be prevented by judicious office/work site configuration.

Misuse of information assets also occurs when CDC computers are used in a manner not intended by the Department.

Examples of incidents of information asset misuse include, but are not limited to:

1. Looking up information on a coworker.

Reading or copying password files, programs, program documentation, or system manuals by a person whose job duties do not require it; use of the information by an unauthorized person to access, or to help an unauthorized

2. person gain access, to computer operating systems, programs, or data.
3. Reading, by an unauthorized individual, information stored on a diskette.
4. Using knowledge of CDC personal or confidential information for non-CDC business reasons.
5. Use of CDC information, by an external CDC information user, for any purpose other than that which was stated and approved.
6. Use of a modem for purposes other than those for which it was approved.
7. Use of an employee's own software on a CDC computer.
8. Bringing and playing games from home on CDC computers.
9. Using a CDC computer for personal business without the approval of the person's supervisor.10) Use of an illegal copy of any software on a CDC computer. Each copy of software on a computer must be part of a CDC site license, network licensing agreement, or purchased by CDC and installed on one computer only. Employees are responsible for knowing and observing all copyright laws for the software they use.

Unauthorized Disclosure

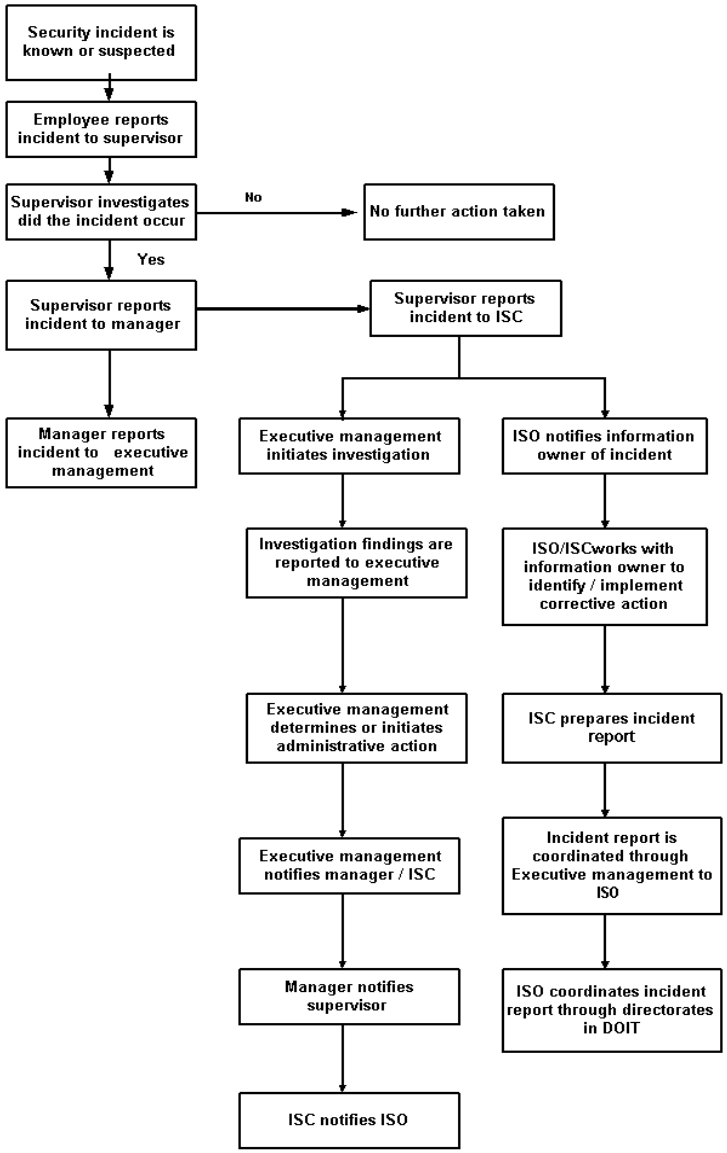
Unauthorized disclosure is release of any CDC information to a person who is not authorized to receive it. This may occur at or away from the work site.

Examples of unauthorized disclosure include, but are not limited to, disclosure by an employee of his or her password. This includes disclosure to family members, coworkers, the employee's supervisor, or any other person. The exception is when the password must be provided to a technician so that maintenance or repairs to the computer or equipment can be

1. made. In these instances, the employee must change his or her password immediately upon completion of the work by the technician.
2. Disclosing another employee's password to anyone. Employees who learn another employee's password should report that fact to their supervisor immediately. The employee must change the password, or if that is not possible, the supervisor must immediately request deactivation of the employee's account by the access management entity.
3. Disclosing medical information or inmate data to any employee whose job does not require this knowledge.
4. Providing address or telephone numbers of a CDC employee or inmate to anyone, including another CDC employee, unless required by CDC.
5. Disclosing to anyone the address of CDC correctional officers or their family members, or other information classified as confidential.
6. Discussing facts from an investigative file or pending legal actions outside the performance of official duties.

Falsification of Information

Falsification of information consists of unauthorized alteration of computerized information, computer programs, or information in any other form. The alteration may be for any reason, including fraud, embezzlement, personal gain, or aiding in the perpetration of a crime or the personal gain of another person. Intentional falsification of computerized data for any reason is in itself a crime under California Penal Code, Section 502. Fraud or other crimes involving information falsification are prosecuted in addition to the crime of computer data falsification.


Security incident is known or suspected
Employee reports incident to supervisor
Supervisor investigates did the incident occur
No
No further action taken
Yes
Supervisor reports incident to manager
Supervisor reports incident to ISC
Manager reports incident to executive management
Executive management initiates investigation
ISO notifies information owner of incident
Investigation findings are reported to executive management
ISO/ISCworks with information owner to identify / implement corrective action
Executive management determines or initiates administrative action
ISC prepares incident report
Executive management notifies manager / ISC
Incident report is coordinated through Executive management to ISO
Manager notifies supervisor
ISO coordinates incident report through directorates in DOIT
ISC notifies ISO